KeyOptions Strategic Advisory Submission - Drone Security Public Consultation Paper 2026

12 MAY 2026

Date: 12 May 2026
11/78 Reserve Road, Artarmon, NSW 2064
www.keyoptions.com

Table of Contents

1. Introduction

KeyOptions welcomes the opportunity to contribute to the Australian Government's development of a modernised drone security framework through the *Drone Security Public Consultation Paper 2026*.

KeyOptions is an Australian company, founded in 1988, specialising in proven and capable counter-unmanned aerial vehicle (C-UAS) systems, command-and-control platforms , UAV solutions and analytics. KeyOptions strongly supports the Government's objective of strengthening drone security while preserving the benefits of legitimate drone use.

2. UAS - The Challenges

The challenge presented by uncrewed systems is no longer one of emerging technology, but of managing a rapidly evolving and increasingly complex threat environment.

Drones are now widely accessible, highly capable and continuously improving. They operate across air, land and maritime domains, and can be adapted quickly for both legitimate and unintended or malicious purposes. The combination of accessibility, capability and adaptability creates a risk profile that is asymmetric, scalable and difficult to predict using traditional regulatory models.

From an operational perspective, the issue is not simply the presence of drones, but the pace and nature of their evolution. Capability is advancing on short cycles, influenced by commercial development and global conflict environments, and is increasingly characterised by autonomy, resilience and reduced reliance on conventional control mechanisms.

This has shifted the environment from isolated incidents to persistent and, in some cases, coordinated activity. It has also exposed the limitations of frameworks that rely primarily on compliance, static rules and device-level controls.

Effective drone security now requires a different approach. It requires the ability to maintain awareness of a dynamic environment, interpret activity in real time, and respond appropriately within operational timeframes.

Australia is now operating in a drone environment where this shift is clearly established. Uncrewed systems are widely available, increasingly capable and easy to adapt, operating across complex environments with reduced reliance on traditional control methods. This has increased both the frequency and complexity of activity, and the challenge of detecting and responding to it effectively.

What is being observed in operational environments is a move beyond occasional misuse toward more deliberate and sustained behaviour. This includes surveillance, disruption,

smuggling and potential payload delivery. The pace of change is being driven by both commercial innovation and lessons learned from operational use overseas. Recent geopolitical developments globally have further accelerated the evolution and use of uncrewed systems. These environments have demonstrated how quickly drone capability can adapt, scale and be applied across varying contexts.

These developments are influencing how governments worldwide are reassessing their approach to drone security. There is a growing recognition that traditional regulatory settings are not sufficient on their own, and that operational capability, integration and the ability to respond in real time are critical.

Internationally, governments are adjusting their approach in a consistent direction. In the United States, Europe and the United Kingdom, registration requirements have been expanded and remote identification frameworks are being implemented as standard or phased in as part of broader efforts. These measures are designed to improve visibility of drone activity as well as strengthen operator accountability and enforcement.

At the same time, these jurisdictions are investing in counter-drone capability and recognising a key limitation. While registration and remote identification improve oversight of compliant users, they do not address the full risk where actors choose not to comply. This reflects a broader shift toward capability-led approaches, where detection, attribution and response are treated as core security functions rather than relying on compliance measures alone.

From an operational perspective, drone security is not primarily a regulatory issue. It is a problem of awareness, attribution and decision-making in real time. The key question is not whether a drone can be detected. It is whether there is enough information, at the right time, to understand what it is, assess intent, identify the operator and determine whether action is required. In most environments, this must occur within very short operational timeframes. Detection without context does not provide a meaningful outcome.

This is why the focus needs to shift from individual technologies to integrated systems. Across any operating environment, multiple sources are generating data. RF monitoring, radar, optical systems and other inputs all provide part of the picture. On their own, they are incomplete and often ambiguous. When properly integrated, they provide a clear and reliable understanding of activity across the environment.

3. Command and Control - The Key to a Layered C-UAS System

Command and Control (C2) systems sit at the centre of this. They are not an optional layer. They are what turns data into decisions. In practice, this means:

- consolidating inputs from multiple sensors into a single operational view
- enabling real-time prioritisation and threat classification
- linking drone activity to operator location and behaviour where detectable
- supporting coordinated and auditable response actions

In operational environments, the value of detection is determined by the quality and usability of the information generated. Systems that can reliably distinguish between known and unknown platforms, identify patterns of behaviour, and reduce false alarms significantly improve operator confidence and response speed.

Experience shows that effective systems are those that can differentiate between legitimate and non-legitimate activity and adapt to previously unseen or modified platforms, rather than relying solely on static libraries or predefined signatures. Without this integration, operators are left managing multiple data feeds with limited context, increasing the likelihood of delayed or incorrect decisions.

A layered approach is equally important. No single technology can address the full spectrum of drone threats. RF detection, radar and optical systems all have strengths, but also clear limitations. These limitations become more pronounced as platforms become more autonomous, operate with reduced RF signatures or are deliberately modified.

A layered system addresses this by combining complementary capabilities. When integrated effectively, this approach provides:

- broader coverage across different threat types
- improved detection confidence through cross-validation
- reduced false alarms
- resilience in complex or degraded environments

Operational deployments consistently show that reliance on a single detection method introduces gaps, particularly in environments with signal congestion, terrain complexity or autonomous flight behaviour. A layered model reduces these gaps by allowing different systems to validate and reinforce each other, improving both coverage and confidence in the operating picture. This becomes increasingly important as platforms evolve toward reduced signal visibility and greater autonomy.

A consistent limitation observed both domestically and internationally is the gap between detection and response. In many cases, systems are able to identify drone activity but there is no clear or timely pathway to act. This may be due to legal constraints, lack of approved mitigation capability, or uncertainty around operational authority.

In high-risk environments such as airports, energy infrastructure or major public events, this is not sustainable. The time between detection and required action is often very short. If

authority and capability are not aligned, the effectiveness of the system is significantly reduced.

Addressing this requires clear, pre-defined frameworks that enable authorised entities to act within controlled parameters, supported by governance, training and appropriate safeguards.

In environments where response is authorised, effectiveness is directly linked to the ability to coordinate detection and intervention within a single workflow. Systems that support real-time alerting, track history, breach notification and response coordination enable faster and more controlled action, while also providing the auditability required for oversight and compliance.

Attribution remains one of the most challenging aspects of drone security. Registration and remote identification provide a useful baseline and should be expanded in line with international practice. They support accountability and improve visibility of compliant users. However, they do not address non-compliant or malicious actors.

In practice, attribution relies on combining multiple sources of information, including:

- registration and remote identification data
- RF detection and direction finding
- behavioural patterns and movement analysis

This approach also enables identification of repeat activity and coordinated behaviour across locations, which is increasingly relevant as drone use becomes more deliberate and persistent. When these inputs are integrated within a single operational system, attribution becomes possible in real time rather than as a post-incident activity.

Another key issue is the fragmentation of data. Drone activity does not sit within a single organisation or jurisdiction. However, the data used to detect and track it often does. This limits the ability to build a complete picture of activity across locations or over time.

A more effective model is a federated approach, where relevant information can be accessed securely by authorised entities while remaining controlled by the originating organisation. This supports a broader operational picture without creating unnecessary complexity.

This is particularly important for identifying patterns over time. Individual incidents may appear low risk in isolation, but when viewed collectively they can indicate persistent surveillance, testing of response thresholds or coordinated activity across multiple sites. Without this level of visibility, activity remains fragmented and the broader intent behind it can be missed.

Preventative measures still have a role. Education, geofencing and registration contribute to safer use and reduce accidental breaches. They support compliant operators and improve general awareness. However, they do not prevent deliberate activity.

Passive detection approaches also support this balance, as they do not interfere with legitimate operations and allow authorities to focus on identifying and responding to genuine threats without impacting compliant users.

There is a risk in relying too heavily on these measures, particularly if they are perceived as providing a level of control that does not exist in practice. Real security outcomes depend on the ability to detect, understand and respond to activity regardless of compliance.

Taken together, these factors point to the need for a shift in how drone security is approached in Australia. Rather than focusing primarily on regulating devices and operators, the framework should be designed as an integrated system. This system should combine layered detection, real-time data integration, reliable attribution and authorised response capability, supported by the ability to share information across relevant stakeholders. It should also be designed to adapt as the threat environment continues to evolve.

In practical terms, this leads to a clear set of priorities:

- expand registration and remote identification in line with international approaches while ensuring they are connected to operational systems
- recognise C2 and data integration as core capability requirements underpinning real-time decision-making
- establish clear, pre-authorised pathways for counter-drone response, supported by governance, training and safeguards
- enable secure and controlled data sharing to support a coordinated view of activity across government, defence and critical infrastructure

Australia is well positioned to take this step. By focusing on integration, capability and adaptability, it can establish a framework that is effective in practice and aligned with how the threat is evolving.

KeyOptions' position is clear. Drone security outcomes will only be achieved through an integrated, layered and data-led approach that supports real-time detection, attribution and response. This approach ensures that investment in capability translates into measurable operational outcomes.

KeyOptions is available to provide further operational insight to support the development of this framework and to ensure that policy settings translate effectively into capability on the ground and in operational environments. Please find our Strategic Recommendations in the following section.

4. KeyOptions Strategic Recommendations

To support the development of an operationally effective and future-ready drone security framework, the following capability considerations are recommended and align with the need for integrated, data-led and operationally focused capability outlined in this submission.

4.1. Integrated Detection and Identification

Detection capability should be able to operate across a wide range of environments and drone types, including commercial, modified and emerging platforms. This includes the ability to:

- identify known and unknown systems
- differentiate between authorised and unauthorised activity
- operate effectively in complex and RF-congested environments

Passive detection approaches should be prioritised where possible, as they enable monitoring without interfering with legitimate operations and reduce the risk of unintended disruption.

4.2. Command and Control (C2) as a Core Capability

A central Command and Control (C2) environment should be treated as a foundational component of any deployment. This should provide:

- a unified operational view across multiple sensors
- real-time alerts for incursions or breaches
- track history and behavioural analysis
- integration of relevant data sources
- audit logging to support oversight and accountability

Such systems should support secure, role-based access and enable use across multiple agencies where required.

4.3. Attribution and Tracking

Operational capability should support real-time tracking and attribution of drone activity. This includes:

- location, movement and flight behaviour
- platform identification where possible
- detection of operator or controller location where feasible
- tracking of multiple drones, including coordinated activity

This level of visibility supports both enforcement and timely decision-making.

4.4. Response Integration

Where response capability is authorised, systems should support integration between detection and mitigation. This includes:

- coordination of response actions within the same operational environment
- clear visibility of response status and outcomes
- full logging of all actions taken

All response activity should be controlled, proportionate and auditable.

4.5. Data Integration and Sharing

Capability should support secure integration and sharing of relevant information across authorised stakeholders. This includes:

- interoperability between systems
- controlled access to operational data
- support for both real-time awareness and historical analysis

This enables improved identification of patterns, repeat activity and emerging threats.

4.6. Deployment and Scalability

Capability should be deployable across a range of environments, including:

- fixed infrastructure locations
- mobile and tactical operations
- urban, regional and remote settings

Systems should be scalable and adaptable to different operational requirements and threat levels.

4.7. Ongoing Adaptation

Given the pace of change in drone capability, systems and frameworks should support ongoing adaptation. This includes:

- regular updates to detection and identification capability
- integration of emerging threat information
- continuous improvement based on operational experience

4.8. Supporting Capability Context

The capability requirements outlined in this submission are supported by mature, operationally deployed systems. By way of practical example, KeyOptions' SkyControl suite and associated C2 platforms illustrate how these requirements can be implemented through an integrated, layered operating model. These systems demonstrate the integration of passive detection, real-time data fusion, attribution and coordinated response within a single operational environment, including:

- passive RF-based detection and identification, including electronic signature analysis
- real-time tracking of drone activity and associated controller location where detectable
- integration of multiple sensor inputs into a unified C2 operating picture
- automated alerting, geofencing and breach notification
- full audit logging of detection, tracking and response activity
- support for role-based access and multi-agency operations

5. Summary

Effective drone security requires capability that can detect, understand, attribute and support authorised response without unnecessarily interfering with legitimate drone activity, while enabling authorities to focus on identifying and responding to genuine threats.

Importantly, these systems also demonstrate how capability can scale across different environments, including fixed infrastructure, mobile deployments and tactical use cases, while maintaining consistency in data, visibility and control.

This reflects the broader principle that effective drone security is not achieved through individual technologies, but through integrated systems that combine detection, attribution and response within a single operational framework.

Date: 12 May 2026
11/78 Reserve Road, Artarmon, NSW 2064
www.keyoptions.com

KeyOptions' experience in deploying and supporting these systems reinforces the importance of aligning policy settings with operational realities, ensuring that capability is both effective and adaptable as the threat environment continues to evolve.